4

INFORMATION CAPACITY OF THE MATCHED GAUSSIAN CHANNEL WITH JAMMING.

I. FINITE-DIMENSIONAL CHANNEL

C.R. Baker* and I.F. Chao**

Department of Statistics
University of North Carolina
Chapel Hill, NC 27599, U.S.A.

Department of Mathematics
Soochow University
Taipei, Taiwan, ROC

LISS-34

April 1989

Abstract

Information capacity is considered for the finite-dimensional additive Gaussian channel subject to jamming. The problem is modeled as a zero-sum two-person game with mutual information as payoff function. The jammer does not control the ambient Gaussian noise, which is not assumed negligible. The unique saddle point and saddle value are determined, along with the jammer's minimax strategy.

Research supported by ONR Grant N00014-86-K-0039 and NSF Grant NCR87137

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for Public Release: Distribution Unlimited
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION Department of Statistics 6b. OFFICE SYMBOL *(If applicable)*	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS *(City, State and ZIP Code)* University of North Carolina Chapel Hill, North Carolina 27514	7b. ADDRESS *(City, State and ZIP Code)*
8a. NAME OF FUNDING/SPONSORING ORGANIZATION Office of Naval Research 8b. OFFICE SYMBOL *(If applicable)*	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER N00014-86-K-0039
8c. ADDRESS *(City, State and ZIP Code)* Statistics & Probability Program Arlington, VA 22217	10. SOURCE OF FUNDING NOS. PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT NO.
11. TITLE *(Include Security Classification)* Information Capacity of the Matched ...	

12. PERSONAL AUTHOR(S)
C.R. Baker and I.F. Chao

13a. TYPE OF REPORT TECHNICAL	13b. TIME COVERED FROM ________ TO ________	14. DATE OF REPORT *(Yr., Mo., Day)* April 1989	15. PAGE COUNT 36

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS *(Continue on reverse if necessary and identify by block number)*
FIELD	GROUP	SUB. GR.	Information capacity, Additive Gaussian channel, Mutual information, Minimax strategy.

19. ABSTRACT *(Continue on reverse if necessary and identify by block number)*

Information capacity is considered for the finite-dimensional additive Gaussian channel subject to jamming. The problem is modeled as a zero-sum two-person game with mutual information as payoff function. The jammer does not control the ambient Gaussian noise, which is not assumed negligible. The unique saddle point and saddle value are determined, along with the jammer's minimax strategy.

11. Title Cont.: Gaussian Channel with Jamming, I. Finite-Dimensional Channel.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT. ☒ DTIC USERS □	21. ABSTRACT SECURITY CLASSIFICATION
22a. NAME OF RESPONSIBLE INDIVIDUAL C.R. Baker	22b. TELEPHONE NUMBER *(Include Area Code)* (919) 962-2189 22c. OFFICE SYMBOL

EDITION OF 1 JAN 73 IS OBSOLETE.

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

1. INTRODUCTION

In the classical additive Gaussian channels, the noise process in the channel is assumed to be fixed and known to the coder. This assumption is frequently not satisfied. One way to approach the capacity problem in such situations is to adopt a game-theoretic formulation with mutual information as the payoff function. This is also a natural approach to modeling the capacity problem when there is an intelligent jammer adding noise to the channel. Such a model was discussed by Blachman (1957) and Dobrushin (1961). However, no substantive results were obtained on this problem until the 1980's. The first paper to obtain such results was apparently that of McEliece and Stark (1981) (see also McEliece (1983), and Borden, Mason and McEliece (1985)). Their model (essentially one-dimensional) deals with the average mutual information $I(X;Y)$ between X and Y, where $Y = X + Z$. X is the channel input, Z the added noise. X and Z are assumed to be independent. The coder controls the input X; X belongs to a class S. The jammer controls the noise Z; Z belongs to a class T. One uses $\Phi(X;Z) \equiv I(X;Y)$ as the payoff function of the game. The coder's program is to find C' such that $C' = \sup_{X\epsilon S} \inf_{Z\epsilon T} \Phi(X;Z)$, and the jammer's program is to find C" such that $C'' = \inf_{Z\epsilon T} \sup_{X\epsilon S} \Phi(X;Z)$. If it happens that $C = C' = C'' = \Phi(X_0,Z_0)$, then (X_0,Z_0) is called a saddle point. Therefore, the framework is based partly on game theory and partly on information theory. McEliece and Stark have shown that under certain restrictions there exist "saddle point" coding and jamming strategies which are simultaneously optimal for both the coder and the jammer.

In this paper, we also adopt the game theory approach. The capacity problem is modeled as a zero-sum two-person game. The payoff function used for this game is the average mutual information. It is assumed that the channel contains an additive ambient Gaussian noise and a hostile additive jamming noise. Thus, the noise added in the channel is partly controlled by an intelligent jammer and partly due to the natural noise, while in the model of McEliece-Stark the noise is completely controlled by the jammer. Both the coder and the jammer are subject to certain energy constraints. In our model, it is assumed that the natural ambient Gaussian noise is known to both the coder and the jammer, and that the coder's constraint is given in terms of the RKHS norm corresponding to the ambient noise. Thus, our model is that of a matched Gaussian channel with jamming. This kind of jamming model is a special case of a mismatched channel. This paper begins with the introduction of the model and the necessary background on optimization methods. The information capacity is then derived for the finite dimensional channel. The solution includes the optimum strategy for the jammer. The solution to the capacity problem for the infinite dimensional channel is given in Baker and Chao (1989).

2. MATHEMATICAL MODEL

The channel to be considered is the matched Gaussian channel with jamming and without feedback. The channel output is $Y = X + N$, where N is a second order noise due to the natural noise W and the independent jamming noise J. It is assumed that they are additive, i.e., $N = W + J$. It will be seen below that the optimal jamming noise J is Gaussian. Therefore it is sufficient to consider the matched Gaussian channel subjected to Gaussian jamming; the channel is then a special type of mismatched Gaussian channel. X is the message process. All stochastic processes considered have their sample paths in $\mathbb{R}^M$. Of course, the results hold for any M-dimensional inner product space. R_W will denote the covariance matrix of W; R_J is the covariance matrix of J. We assume WLOG that R_W is strictly positive. We use $\mathbb{R}^M$ interchangeably to denote both the space $\mathbb{R}^M$ and the M-dimensional inner product space $(\mathbb{R}^M, \langle\cdot,\cdot\rangle)$, $\langle u,v\rangle = \Sigma_{i-1}^M u_i v_i$.

2.1. Bounds on Information Capacity

Let P_1 and P_2 be two probability measures defined on the same measurable space $(\Omega,\mathcal{F})$. The entropy $H_{P_2}(P_1)$ of P_1 with respect to P_2 is defined by $H_{P_2}(P_1) = \sup \Sigma_i P_1(C_i)[\log(P_1(C_i)/P_2(C_i))]$ where the supremum is taken over all finite measurable partitions (C_i) of Ω. We consider a message process X defined by a probability μ_X on the Borel sets $\mathcal{B}[\mathbb{R}^M]$, with the observation, noise, and transmitted signal processes all defined by probabilities on $\mathcal{B}[\mathbb{R}^M]$. $\|\cdot\|$ will denote the norm obtained from the usual inner product $\langle\cdot,\cdot\rangle$ on $\mathbb{R}^M$. Let μ_N be a noise on $\mathcal{B}[\mathbb{R}^M]$ which is not necessarily Gaussian. Assume μ_N is second order. Let $\mathcal{K}$ be a class of covariance matrices on $\mathbb{R}^M$. Let $\mathcal{X}$ be the class of second order probabilities μ_X on $\mathcal{B}[\mathbb{R}^M]$ having a covariance matrix belonging to $\mathcal{K}$. $\mathcal{X}$ represents a class of allowable input distributions determined by their covariance operators.

Lemma 1 (Ihara (1978)): Let μ_{N^o} be a zero-mean Gaussian measure on $\mathcal{B}[\mathbb{R}^M])$ having the same covariance matrix as μ_N. Then

$$\mathcal{C}(\mu_{N^o},\mathcal{X}) \leq \mathcal{C}(\mu_N;\mathcal{X}) \leq \mathcal{C}(\mu_{N^o};\mathcal{X}) + H_{\mu_{N^o}}(\mu_N)$$

where $\mathcal{C}(\mu_N;\mathcal{X}) = \sup\{I(X,Y)\colon X\in\mathcal{X}\}$, $Y = X + N$ and $I(X,Y)$ denotes the mutual information between the input X and the output Y.

Remark: Ihara's result shows that the information capacity can be decreased by choosing Gaussian noise among a class of second order processes having the same covariance matrix. We thus assume henceforth that the jamming noise is Gaussian.

2.2. Gaussian Channel With Jamming

Let H_W be the RKHS for the covariance matrix R_W, with norm $\|\cdot\|_W$, defined by $\|x\|_W = \|R_W^{-1/2}x\|^2$. It should be noted that the elements of H_W consist of all of $\mathbb{R}^M$. In this finite-dimensional case, one could replace $\|\cdot\|_W$ with $\|\cdot\|$ while replacing N with $R_W^{-1/2}N$ and J with $R_W^{-1/2}J$. The $\|\cdot\|_W$ norm is used because of the extension to infinite-dimensional Hilbert space considered in Baker and Chao (1989), where the RKHS H_W will not consist of all elements of the Hilbert space.

Let S be the covariance matrix defined by $S = R_W^{-1/2}R_JR_W^{-1/2}$, so that $R_N = R_W + R_J = R_W^{1/2}(I+S)R_W^{1/2}$.

The constraint for the coder is $$E_{\mu_X}\|X\|_W^2 \leq P_1. \qquad (1)$$

Under the constraint (1), let $C_W(P_1) = \sup_Q I[\mu_{XY}]$. Q is the set of μ_X that satisfy (1).

From the results of Baker (1978), one can limit attention to the case where μ_X is Gaussian with covariance $R_X = \Sigma\, \tau_n[R_N^{1/2}u_n] \otimes [R_N^{1/2}u_n]$, where $\tau_n \geq 0$, $n \geq 1$, $\Sigma_n\tau_n < \infty$, $\{u_n, n\geq 1\}$ is a CONS and $(u\otimes v)x \equiv \langle v,x\rangle u$. Then $I[\mu_{XY}] = \frac{1}{2}\Sigma_n\log(1+\tau_n)$. Moreover, $E_{\mu_X}\|X\|_W^2 = E_{\mu_X}\|R_W^{-1/2}A(X)\|^2 = TrR_W^{-1/2}R_XR_W^{-1/2} = \Sigma\,\tau_n\|(I+S)^{1/2}U^*u_n\|^2 \leq P_1$. Suppose now that S is fixed. Setting $z_n = \tau_n\|(I+S)^{1/2}U^*u_n\|^2$, $C_W(P) = \sup (1/2)\,\Sigma_n \log(1+z_n(1+\gamma_n)^{-1})$ where the supremum is over the sequences (z_n) and CONS $\{v_n, n\geq 1\}$ in $\mathbb{R}^M$ such that $\Sigma_n z_n \leq P_1$, and $\gamma_n = \langle Sv_n, v_n\rangle$, $n\geq 1$. Here, $v_n = U^*u_n$.

The quantity of interest is $I[\mu_{XY}]$. As seen, it is a function of (τ_n) and (z_n), defined as above. Henceforth, we make this explicit by defining

$$F(z,\tau) = (\tfrac{1}{2}) \sum_n \log\left[1 + z_n(1+\tau_n)^{-1}\right]$$

where (z_n) and $(\tau_n\}$ are defined above.

In general, $\sup_z \inf_\tau F(z,\tau) \leq \inf_\tau \sup_z F(z,\tau)$ (see, e.g., Barbu and Precupanu (1986)). Equality can hold in this relation without the common value being attained by a point (z^*,τ^*). If equality does hold, we say that the game has a *saddle value*. The value is attained if and only if there exists an admissible point (z^*,τ^*) such that

$$\sup_z F(z,\tau^*) \leq F(z^*,\tau^*) \leq \inf_\tau F(z^*,\tau).$$

The point (z^*,τ^*) is then said to be a *saddle point* for F, and of course $F(z^*,\tau^*)$ is the saddle value. Existence of a saddle point must be shown, even if a saddle value exists. When a saddle point does exist, then obviously $\sup_z$ and $\inf_\tau$ in the above inequalities (which is then an equality) can be replaced by $\max_z$ and $\min_\tau$.

Of course, the existence and definition of a saddle point for F depend on the class of admissible points (z,τ). We have already defined the admissible z as those non-negative real-valued sequences satisfying $\Sigma_{n\geq 1} z_n \leq P_1$, where $P_1 \geq 0$ is fixed. We now discuss the class of admissible τ.

The constraint $\Sigma_{n\geq 1} z_n \leq P_1$ on the coder is equivalent to the constraint $E_{\mu_X} \|x\|_W^2 \leq P_1$. That is, $z_n = \tau_n \|(I+S)^{\frac{1}{2}} U^* u_n\|^2$, where $\{u_n, n\geq 1\}$ is any CONS in

$\mathbb{R}^M$, U is the unitary operator defined above, and the coder has covariance matrix $R_X = \Sigma_n \tau_n R_N^{\frac{1}{2}} u_n \otimes R_N^{\frac{1}{2}} u_n$.

A constraint that one might naturally assume for the jammer would be of a similar nature: $E_{\mu_J} \|x\|_W^2 \leq P_2$. This is the same as Trace S $\leq P_2$, since $R_J = R_W^{\frac{1}{2}} S R_W^{\frac{1}{2}}$. Suppose that one considers the infinite-dimensional channel. Since S is then trace class, it has zero as the only limit point of its spectrum. Examining the expression for channel capacity given in Theorem 3 of of Baker (1987), one sees that for the infinite-dimensional channel, such a constraint would not enable the jammer to decrease the capacity. This holds for any value of P_2, no matter how large. Thus, in the infinite-dimensional channel, the jammer must have a constraint that is of a weaker form than that for the coder. However, in the finite-dimensional channel, we shall see that the saddle point solution for this constraint is a special case of the constraint we use.

The constraint to be applied on the jammer is $E_{\mu_J} \|x\|^2 \leq P_2$. It will be seen that such a constraint provides a well-defined game-theoretic problem, and it can be seen to be not unreasonable from a physical viewpoint. This constraint can be written in terms of the covariance matrix R_J of J: Trace $R_J \leq P_2$. Using the fact that $R_J = R_W^{\frac{1}{2}} S R_W^{\frac{1}{2}}$, as discussed above, the jammer's constraint becomes Trace $R_W^{\frac{1}{2}} S R_W^{\frac{1}{2}} \leq P_2$.

Let $\{e_n, n \geq 1\}$ be the CONS of eigenvectors of R_W, (λ_n) the corresponding eigenvalues, and suppose that $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n \geq \ldots$. Our constraint on the jammer is that Trace $R_J \leq P_2$. Thus,

$$P_2 \geq \mathrm{Tr} R_J = \mathrm{Tr} R_W^{\frac{1}{2}} S R_W^{\frac{1}{2}} = \sum_1^\infty \langle S R_W^{\frac{1}{2}} e_n, R_W^{\frac{1}{2}} e_n \rangle = \sum_1^\infty \lambda_n \langle S e_n, e_n \rangle.$$

The basic problem can now be summarized as follows. $F(z,\tau) = \frac{1}{2}\sum_{n\geq 1}\log[1+z_n(1+\tau_n)^{-1}]$, where $z_n \geq 0$ and $\tau_n \geq 0$ for $n \geq 1$, and $\Sigma z_n \leq P_1$. (z_n) is selected by the coder, $z_n = \tau_n\|(I+S)^{\frac{1}{2}}U^* u_n\|^2$, where $\{u_n, n\geq 1\}$ is a CONS for $\mathbb{R}^M$, and the coder chooses the covariance matrix $R_X = \Sigma_{n\geq 1}\tau_n R_N^{\frac{1}{2}}u_n \otimes R_N^{\frac{1}{2}}u_n$, with $R_N = R_W + R_J$. The jammer chooses his covariance matrix $R_J = R_W^{\frac{1}{2}}SR_W^{\frac{1}{2}}$, subject to the constraint $\Sigma_{n\geq 1}\lambda_n\langle Se_n, e_n\rangle \leq P_2$, where $R_W = \lambda_n e_n \otimes e_n$. The sequence (τ_n) is then defined by $\tau_n = \langle Sv_n, v_n\rangle$, where $v_n = U^* u_n$, $1 \leq n \leq M$.

The problem as formulated does not explicitly exhibit a constraint on (τ_n). This apparent ambiguity will be removed as part of the analysis.

2.3. Optimization And Minimax Theorems

Here we summarize fundamental theorems to be applied to our problem.

Lemma 2 (Danskin (1967)): Suppose that the set $x = (x_1,\ldots,x_n)$ maximizes $\Sigma f_i(y_i)$ subject to the side condition $\Sigma y_i = X$, $y_i \geq 0$. Suppose that f_i are differentiable. Then there exists a λ such that

$$f_i'(x_i) = \lambda \quad \text{if } x_i > 0$$

$$f_i'(x_i) \leq \lambda \quad \text{if } x_i = 0.$$

Lemma 3 (Roberts and Varberg (1973)): Let $f\colon U \to R$ be convex on a convex set $U \subset L$, where L is a normed linear space. If f has a local minimum at $\bar{x}$, then $f(\bar{x})$ is also a global minimum. The set V on which f attains its minimum is convex. If f is strictly convex in a neighborhood of a minimum point $\bar{x}$, then $V = \{\bar{x}\}$; that is, the minimum point is unique.

Lemma 4 (Barbu and Precupanu (1986)): (general von Neumann minimax theorem). Let L_1 and L_2 be reflexive Banach spaces, with $U \subset L_1$ and $V \subset L_2$ two nonempty bounded, closed, and convex subsets. Let f: U×V → ℝ. Suppose that for each fixed y, f(x,y) is continuous and concave on U and that for each fixed x, f(x,y) is continuous and convex on V. Then there is a saddle point $(\bar{x},\bar{y})$ for f on U×V and

$$\max_{x\in U}\min_{y\in V} f(x,y) = \min_{y\in V}\max_{x\in U} f(x,y) = f(\bar{x},\bar{y}).$$

Remark: For the finite-dimensional channel, we shall see that F and the constraint conditions for z and τ satisfy the sufficient conditions of Lemma 4. Therefore, there exists a unique saddle point (z^{o},τ^{o}).

3. INFORMATIOM CAPACITY WITH JAMMING

3.1. Preliminary Results

Lemma 5 (Baker (1987)): Suppose that the jammer's strategy is fixed, given by (τ_i) where $0 \leq \tau_1 \leq \tau_2 \leq \dots \leq \tau_M$. Then the maximal value of $F(z,\tau)$, denoted by $F_0(\tau)$, is given by

$$F_0(\tau) = \tfrac{1}{2}\sum_{1}^{K} \log\left[\frac{P_1+\Sigma_1^K\tau_i+K}{(1+\tau_i)K}\right]$$

where K is the largest integer such that $P_1 + \Sigma_1^K\tau_i \geq K\tau_K$, and the coder's optimun strategy is to select z_i as follows:

$$z_i = C - \tau_i = \frac{P_1+\Sigma_{j=1}^K\tau_j}{K} - \tau_i,\ i=1,2,\dots,K,\ \text{with } z_i = 0,\ i = k+1,\dots,M.$$

Moreover, the maximum is uniquely attained when the coder chooses a Gaussian signal process with measure μ_X and covariance operator $R_X = \Sigma_{i=1}^K z_i(1+\tau_i)R_N^{\frac{1}{2}}u_i \otimes R_N^{\frac{1}{2}}u_i$, where $S = \Sigma_{i=1}^M \tau_i v_i \otimes v_i$, $v_i = U^* u_i$ for $1 \leq i \leq M$, and

$\{u_n, n \geq 1\}$ is a CONS for H_2.

In the finite-dimensional channel, we are dealing with (z,γ) contained in $\mathbb{R}^M \times \mathbb{R}^M$. W? wish to apply Lemma 4 to guarantee existence of a saddle point for F. ?owever, F is given in terms of (γ_n), where $\gamma_n = \langle SU^* u_n, U^* u_n \rangle$, and $\{u_n, n \geq 1\}$ is selected by the coder. The constraint on the jammer is given by $\Sigma_n \lambda_n \langle Se_n, e_n \rangle \leq P_2$. This constraint needs to be expressed in terms of (γ_n) in order that Lemma 4 can be applied. This is obtained from the following result.

Lemma 6: Without loss of generality, the jammer's minimax strategy can be achieved by taking $S = \Sigma_{i=1}^M \gamma_i e_i \otimes e_i$, where $\Sigma_{i=1}^M \lambda_i \gamma_i \leq P_2$, $\gamma_i \geq 0$ for $i \leq M$.

Proof: In general, the jammer wishes to select γ in order to minimize F_0, as defined above. He selects $S = \Sigma_{n \geq 1} \gamma_n U^* u_n \otimes U^* u_n$, where $\{u_n, n \geq 1\}$ is a CONS for H_2, subject to the constraint $\Sigma_{i \geq 1} \lambda_i \langle Se_i, e_i \rangle \leq P_2$, where $R_W = \Sigma_{i \geq 1} \lambda_i e_i \otimes e_i$.

Since the value of $F_0(\gamma)$ depends only on the choice of (γ_n) and not on the choice of $\{u_n, n \geq 1\}$, it is sufficient to prove that if $S = \Sigma_{i \geq 1} \gamma_i v_i \otimes v_i$, where $\{v_i, i < M\}$ is any CONS in $\mathbb{R}^M$, then $\Sigma_{i \geq 1} \lambda_i \langle Se_i, e_i \rangle \geq \Sigma_{i \geq 1} \lambda_i \gamma_i$. If this inequality is satisfied, then any choice of (γ_n) and $\{u_n, n \geq 1\}$ satisfying the constraint $\Sigma_{i \geq 1} \lambda_i \langle Se_i, e_i \rangle \leq P_2$ will provide a value of F_0 which is also obtained by an admissible operator $S' \equiv \Sigma_{i \geq 1} \gamma_i e_i \otimes e_i$, since $\Sigma \lambda_i \langle S' e_i, e_i \rangle = \Sigma \lambda_i \gamma_i$.

Thus, to complete the proof it is sufficient to show that $\Sigma_{i=1}^M \lambda_i \langle Se_i, e_i \rangle \geq \Sigma_{i=1}^M \lambda_i \gamma_i$.

Let $\{v_i, 1 \leq i \leq M\}$ be the CONS of the eigenvectors of S and $\{\gamma_i, 1 \leq i \leq M\}$ be the corresponding eigenvalues. Assume $\gamma_1 \leq \gamma_2 \leq \cdots \leq \gamma_M$.

Consider $$v_i = \sum_{j=1}^{M} \langle v_i, e_j \rangle e_j, \qquad e_i = \sum_{j=1}^{M} \langle e_i, v_j \rangle v_j$$

$$\|v_i\|^2 = \sum_{j=1}^{M} \langle v_i, e_j \rangle^2 = 1 \qquad \|e_j\|^2 = \sum_{j=1}^{M} \langle e_i, v_j \rangle^2 = 1$$

Define $a_{ij} = \langle v_i, e_j \rangle$; then $\sum_{i=1}^{M} a_{ij}^2 = \sum_{j=1}^{M} a_{ij}^2 = 1$, and

$$\mathrm{Tr} R_W^{\frac{1}{2}} S R_W^{\frac{1}{2}} = \mathrm{Tr} R_W S = \sum_{i=1}^{M} \langle R_W S v_i, v_i \rangle = \sum_{i=1}^{M} \langle R_W \gamma_i v_i, v_i \rangle$$

$$= \sum_{i=1}^{M} \langle \sum_{j=1}^{M} a_{ij} \lambda_j e_j, \sum_{k=1}^{M} a_{ik} e_k \rangle \gamma_i = \sum_{i=1}^{M} \sum_{j=1}^{M} a_{ij}^2 \lambda_j \gamma_i .$$

To complete the proof of the lemma, it is now sufficient to obtain the following equality:

$$\inf_{A=[a_{ij}]} \sum_{i=1}^{M} \sum_{j=1}^{M} \lambda_j a_{ij}^2 \gamma_i = \sum_{i=1}^{M} \lambda_i \gamma_i$$

where $A = [a_{ij}]$ is a real unitary matrix. This equality has been proved by Fan (1951). □

We have now reformulated the original problem into the following form. The payoff function is F, defined on $\mathbb{R}^M \times \mathbb{R}^M$,

$$F(z, \gamma) = \tfrac{1}{2} \sum_{i=1}^{M} \log\left[1 + z_n (1+\gamma_n)^{-1}\right]$$

where $z \in U$, $\gamma \in V$,

$$U = \{z \text{ in } \mathbb{R}^M: z_i \geq 0 \text{ for } i \leq M, \sum_{i=1}^{M} z_i \leq P_1\}$$

$$V = \{\gamma \text{ in } \mathbb{R}^M: \gamma_i \geq 0 \text{ for } i \leq M, \sum_{i=1}^{M} \lambda_i \gamma_i \leq P_2\}.$$

In this form, F,U, and V satisfy the conditions of Lemma 4, so that a saddle point is guaranteed to exist for F on U×V. Moreover, the saddle point is obtained by minimizing the function F_0 with respect to γ, and defining z as in the beginning of this subsection (as in Lemma 5). This will be the problem to be considered in the remainder of this section.

It should be emphasized that this means that the coder and the jammer always use the $\{e_n, n \geq 1\}$. They are o.n. eigenvectors of S, and the coder uses the covariance matrix $R_X = \Sigma_{n\geq 1}\gamma_n(1+\gamma_n)\lambda_n e_n \otimes e_n$, where $\Sigma_{n\geq 1}\gamma_n(1+\gamma_n) \leq P_1$, and $\Sigma_{n\geq 1}\gamma_n\lambda_n \leq P_2$.

We now obtain an important condition in order that (z,γ) define a saddle point.

Lemma 7: The saddle point (z,γ) of F must satisfy the following condition: If $\gamma_0 = \max\{\gamma_1,\ldots,\gamma_M\}$, then

$$P_1 + \sum_{i=1}^{M} \gamma_i \geq M\gamma_0 \qquad (M \geq 2).$$

Proof: Our constraint on (γ_i) is $\Sigma_{i=1}^{M}\lambda_i\gamma_i \leq P_2$. The (λ_i) are defined to be non-increasing: $\lambda_{i+1} \leq \lambda_i$, $i \leq M-1$. For the proof, we will re-order the (λ_i) and (γ_i), if necessary, in such a way that (γ_i) is non-decreasing. Hence, in the proof to follow, we make this assumption; we do not assume that (λ_i) is non-increasing; the reordered sequence is denoted by (λ_i^o). From Lemma 5, this ordering then requires that (z_i) be non-increasing. Now, given the original saddle point (z^o, γ^o), which fixes the indices of (λ_n^o), we require that any admissible point (z, γ) also satisfy (γ_n) non-decreasing, (z_n) non-increasing.

If the lemma is false, then there exists $K < M$, such that $K\gamma_{K+1}^o > P + \Sigma_1^K \gamma_i^o \geq K\gamma_K^o$, and (z^o, γ^o) is a saddle point of F with

$$\gamma^o = (\gamma_1^o, \gamma_2^o, \ldots, \gamma_M^o);\ 0 \leq \gamma_i^o \leq \gamma_2^o \leq \cdots \leq \gamma_M^o;\ \Sigma_1^M \lambda_i \gamma_i^o \leq P_2.$$

$$z^o = (z_1^o, z_2^o, \ldots, z_M^o);\ z_1^o \geq z_2^o \geq \cdots \geq z_K^o \geq 0.$$

$$z_i^o = 0,\ i = K+1, \ldots, M,\ \Sigma_1^K z_i^o = P_1.$$

Moreover, $z_K^o = 0$ if and only if $\sum_{i=1}^{K} \gamma_i^o + P_1 = K\gamma_K^o$.

First, suppose that $\sum_{i=1}^{K} \gamma_i^o + P_1 = K\gamma_K^o$. Choose $\epsilon > 0$ such that $\epsilon < (\gamma_{K+1}^o - \gamma_K^o)/2$ and $\epsilon < \lambda_K(\gamma_{K+1}^o - \gamma_K^o)/(2\lambda_{K+1}^o)$. Define a new jamming sequence (γ_i^*) by

$$\gamma_i^* = \gamma_i^o, \qquad i \neq K,\ K+1$$

$$\gamma_K^* = \gamma_K^o + \epsilon\, \lambda_{K+1}^o / \lambda_K^o$$

$$\gamma^*_{k+1} = \gamma_{K+1}^o - \epsilon.$$

Then $\sum_{i=1}^{K} \gamma_i^* + P_1 < K\gamma_K^*$, and by Lemma 5,

$$F_0(\gamma^*) = \tfrac{1}{2} \sum_{i=1}^{K-1} \log\left[\frac{P_1 + \Sigma_{j=1}^{K-1} \gamma_j^o + K-1}{(K-1)(1+\gamma_i^o)}\right].$$

Again applying Lemma 5, $F_0(\gamma^*) < F_0(\gamma^o)$. Moreover, the sequence (γ_i^*) is admissible; $\gamma_i^* \leq \gamma_{i+1}^*$ for $i \leq M-1$ (so that the conditions of Lemma 5 are satisfied), and

$$\sum_{i=1}^{M} \lambda_i \gamma_i^{*} = \sum_{i=1}^{M} \lambda_i \gamma_i^{\circ} + \lambda_K[\epsilon\lambda_{K+1}/\lambda_K] - \lambda_{K+1}\epsilon = \sum_{i=1}^{M} \lambda_i \gamma_i^{\circ} \le P_2.$$

Next, suppose that $P_1 + \sum_{i=1}^{K} \gamma_i^{\circ} > K\gamma_K^{\circ}$.

We then consider the derivative of F_0 with respect to γ_K°; this is equal to $\frac{1}{2}\left[\frac{K}{P_1+K+\Sigma_{j=1}^{K}\gamma_j^{\circ}} - \frac{1}{1+\gamma_K^{\circ}}\right]$. This derivative is strictly negative, since $K(1+\gamma_K^{\circ}) < P_1 + K + \Sigma_{j=1}^{K}\gamma_j^{\circ}$. It follows that if we can define an admissible sequence (γ_n^{*}) such that γ_n^{*} differs from (γ_n°) only for the indices K and K+1, with $\gamma_K^{*} > \gamma_K^{\circ}$ and satisfying $K\gamma_{K+1}^{*} > \sum_{i=1}^{K} \gamma_i^{*} + P_1 \ge K\gamma_K^{*}$, then $F_0(\gamma^{*}) < F_0(\gamma^{\circ})$. This will then contradict $(z^{\circ},\gamma^{\circ})$ being the saddle point.

Thus, let β be such that $\beta < (\gamma_{K+1}^{\circ}-\gamma_K^{\circ})/2$, $\lambda_{K+1}^{\circ}\beta/\lambda_K^{\circ} < (\gamma_{K+1}^{\circ}-\gamma_K^{\circ})/2$, $\lambda_{K+1}^{\circ}\beta/\lambda_K^{\circ} < \left[P_1+\Sigma_{i=1}^{K}\gamma_i^{\circ}-K\gamma_K^{\circ}\right]/(K-1)$, and $\beta < \left[K\gamma_{K+1}^{\circ}-P_1-\Sigma_{i=1}^{K}\gamma_i^{\circ}\right]/(K+\lambda_{K+1}^{\circ}/\lambda_K^{\circ})$. Note that $\gamma_{K+1}^{\circ} > \gamma_K^{\circ}$ is necessary, by the definition of K.

Let $\epsilon = \lambda_{K+1}^{\circ}\beta/\lambda_K^{\circ}$. Now define (γ_i^{*}) by

$$\gamma_i^{*} = \gamma_i^{\circ}, \quad i \neq K,\ i \neq K+1$$

$$\gamma_K^{*} = \gamma_K^{\circ} + \epsilon$$

$$\gamma_{K+1}^{*} = \gamma_{K+1}^{\circ} - \beta.$$

As shown above, $F_0(\gamma^{*}) < F_0(\gamma^{\circ})$, since $K\gamma_{K+1}^{*} > P_1 + \Sigma_{i=1}^{K}\gamma_i^{*} \ge K\lambda_K^{*}$. To see the last inequality, one notes that $\Sigma_{i=1}^{K}\gamma_i^{*} + P_1 = \Sigma_{i=1}^{K}\gamma_i^{\circ} + P_1 + \epsilon \ge K(\gamma_K^{\circ}+\epsilon) = K\gamma_K^{*}$. The inequality $K\gamma_{K+1}^{*} > P_1 + \Sigma_{i=1}^{K}\gamma_i$ can be seen similarly:

$$K(\gamma_{K+1}^{*}-\gamma_K^{*}) = K(\gamma_{K+1}^{\circ}-\gamma_K^{\circ}) - K(\beta+\epsilon),$$

and $$K\beta + \epsilon < K\overset{\circ}{\gamma}_{K+1} - P_1 - \sum_{i=1}^{K} \overset{\circ}{\gamma}_i ,$$

so $$K(\gamma^*_{K+1} - \gamma^*_K) > K(\overset{\circ}{\gamma}_{K+1} - \overset{\circ}{\gamma}_K) - K\overset{\circ}{\gamma}_{K+1} + P_1 + \sum_{i=1}^{K} \overset{\circ}{\gamma}_i - (K-1)\epsilon ,$$

$$K\gamma^*_{K+1} > P_1 + \sum_{i=1}^{K} \overset{\circ}{\gamma}_i + K(\gamma^*_K - \overset{\circ}{\gamma}_K) - (K-1)\epsilon .$$

Since $\gamma^*_K - \overset{\circ}{\gamma}_K = \epsilon$, the last inequality gives

$$K\gamma^*_{K+1} > P_1 + \sum_{i=1}^{K} \overset{\circ}{\gamma}_i + \epsilon = P_1 + \sum_{i=1}^{K} \gamma^*_i .$$

It remains to show that (γ^*_i) is an admissible strategy for the jammer. First, (γ^*_i) is non-decreasing, since

$$\overset{\circ}{\gamma}_K + \epsilon < \overset{\circ}{\gamma}_K + \frac{(\overset{\circ}{\gamma}_{K+1} - \overset{\circ}{\gamma}_K)}{2} = \frac{(\overset{\circ}{\gamma}_{K+1} + \overset{\circ}{\gamma}_K)}{2}$$

and $$\overset{\circ}{\gamma}_{K+1} - \beta > \overset{\circ}{\gamma}_{K+1} - \frac{(\overset{\circ}{\gamma}_{K+1} - \overset{\circ}{\gamma}_K)}{2} = \frac{(\overset{\circ}{\gamma}_{K+1} + \overset{\circ}{\gamma}_K)}{2} .$$

Moreover, $\sum_{i=1}^{M} \overset{\circ}{\lambda}_i \gamma^*_i = \sum_{i=1}^{M} \overset{\circ}{\lambda}_i \overset{\circ}{\gamma}_i + \overset{\circ}{\lambda}_K \epsilon - \overset{\circ}{\lambda}_{K+1} \beta = \sum_{i=1}^{M} \overset{\circ}{\lambda}_i \overset{\circ}{\gamma}_i \le P_2$.

The sequence (γ^*_i) is thus non-decreasing and satisfies the jammer's constraint, so is an admissible strategy. □

Remark. The content of Lemma 7 is that the jammer's optimum strategy includes forcing the coder to spread his available energy across the entire channel (i.e., the coder cannot restrict his signal to any proper subset of $\mathbb{R}^M$).

Lemma 8: Suppose that the jammer's strategy is given by (γ_i). If there exists K such that $\lambda_K > \lambda_{K+1}$ and $\gamma_K > \gamma_{K+1}$, then (γ_i) is not a minimax strategy.

Proof: From Lemma 5 and Lemma 7, in order to achieve $\sup_z F(z,\gamma)$ the coder must have (z_i) defined by

$$z_k = \frac{P_1 + \Sigma_{i=1}^{M}\gamma_i}{M} - \gamma_k, \quad k = 1,2,\ldots,M.$$

We consider

$$F_0(\gamma) = \tfrac{1}{2}\sum_{i=1}^{M} \log\left[\frac{P_1+\Sigma_{j=1}^{M}\gamma_j+M}{M(1+\gamma_i)}\right].$$

Note that the ordering of (γ_i) does not affect the value of $F_0(\gamma)$, since all M γ_i's are used.

We have $\Sigma_1^M\lambda_i\gamma_i \le P_2$. Define a new sequence (γ_i^*) as follows:

$$\gamma_i^* = \gamma_i \qquad i \neq K,\ i \neq K+1$$

$$\gamma_K^* = \gamma_{K+1} + \epsilon$$

$$\gamma_{K+1}^* = \gamma_K$$

where $\epsilon > 0$ is such that $\gamma_{K+1} + \epsilon < \gamma_K$ and $\lambda_K(\gamma_{K+1}+\epsilon) + \lambda_{K+1}\gamma_K \le \lambda_K\gamma_K + \lambda_{K+1}\gamma_{K+1}$. We first show that $F_0(\gamma^*) < F_0(\gamma)$. First, by Lemma 6, if (γ_i) is a minimax strategy, then $P_1 + \Sigma_{i=1}^M\gamma_i \ge M\gamma_0$, where $\gamma_0 = \max\{\gamma_1,\ldots,\gamma_M\}$. Since $\gamma_K^* = \gamma_{K+1} + \epsilon < \gamma_K \le \gamma_0$, $P_1 + \Sigma_{i=1}^M\gamma_i^* = P_1 + \Sigma_{i=1}^M\gamma_i + \epsilon > P_1 + \Sigma_{i=1}^M\gamma_i \ge M\gamma_0 = M\gamma_0^*$, $\gamma_0^* = \max\{\gamma_1^*,\ldots,\gamma_M^*\}$. As in the proof of Lemma 7, $F_0(\gamma^*) < F_0(\gamma)$, since $\{\gamma_1^*,\ldots,\gamma_M^*\} = \{\gamma_i,\ i \neq K+1\} \cup \{\gamma_{K+1} + \epsilon\}$, and $F_0(\gamma)$ is a non-increasing function of γ_i for any fixed $i \le M$. This shows that (γ_n) is not a minimax strategy for the jammer, providing that (γ_n^*) is admissible.

To complete the proof, we need to define $\epsilon > 0$ such that $\Sigma_{i=1}^M\lambda_i\gamma_i^* \le P_2$. Note that $\Sigma_1^M\lambda_i\gamma_i - \Sigma_1^M\lambda_i\gamma_i^* = \lambda_K(\gamma_K-\gamma_{K+1}) - \lambda_K\epsilon + \lambda_{K+1}(\gamma_{K+1}-\gamma_K) = (\lambda_K-\lambda_{K+1})(\gamma_K-\gamma_{K+1}) - \lambda_K\epsilon$. Let $\epsilon \le (\lambda_K-\lambda_{K+1})(\gamma_K-\gamma_{K+1})/\lambda_K$. Then

$\Sigma_1^M\lambda_i\gamma_i^* \leq \Sigma_1^M\lambda_i\gamma_i = P_2$, while $F_0(\gamma^*) < F_0(\gamma)$. □

Henceforth we shall assume without loss of generality that (γ_i) is non-decreasing (so that (z_i) is non-increasing).

Lemma 9: Define

$$\Lambda = \{(z,\gamma)\colon 0 \leq \gamma_1 \leq \gamma_2 \leq \dots \leq \gamma_M,\ \Sigma_1^M\lambda_i\gamma_i \leq P_2,$$

$$z_1 \geq z_2 \geq z_3 \geq \dots \geq z_M \geq 0,\ \Sigma_1^M z_i \leq P_1\},$$

and

$$\bar{\Lambda}_K = \{(z,\gamma)\colon 0 = \gamma_1 = \dots = \gamma_K \leq \gamma_{K+1} \leq \dots \leq \gamma_M,\ \Sigma_1^M\lambda_i\gamma_i \leq P_2,$$

$$z_1 \geq z_2 \geq \dots \geq z_K \geq z_{K+1} \geq \dots \geq z_M \geq 0,\ \Sigma_1^M z_i \leq P_1\}.$$

For $K \leq M$, define C_K by $\underset{(z,\gamma)\epsilon\bar{\Lambda}_K}{\min_{\gamma}\max_{z}} F(z,\gamma)$. The saddle point (z,γ) then belongs to $\Lambda_K = \bar{\Lambda}_K - \bar{\Lambda}_{K+1}$ where K is the smallest integer such that $C_K < C_{K+1}$. If $C_1 = C_2 = \dots = C_M$, then the saddle point belongs to Λ_M.

Proof: $\bar{\Lambda}_K$ is compact and convex for all K, $0 \leq K \leq M-1$. $\bar{\Lambda}_0 \supset \bar{\Lambda}_1 \supset \dots \supset \bar{\Lambda}_{M-1}$. $\bar{\Lambda}_0 = \Lambda$. C_K is well-defined, by Lemma 4, and $C_K \leq C_{K+1}$, $0 \leq K \leq M-1$. Moreover, $\Lambda_K = \bar{\Lambda}_K - \bar{\Lambda}_{K+1}$ and Λ_K are disjoint. Let $C_K \equiv F(z_K,\gamma_K)$, then (z_0,γ_0) is the saddle point for Λ. To complete the proof, one notes that a unique saddle point (z_K,γ_K) exists in each of the sets $\bar{\Lambda}_K$, by Lemma 4.

If $C_K = C_{K+1}$, then applying Lemma 3 to the strictly convex function F_0, one must have $(z_K,\gamma_K) = (z_{K+1},\gamma_{K+1})$; i.e., the saddle point for $\bar{\Lambda}_K$ is the saddle point for $\bar{\Lambda}_{K+1}$. If $C_K < C_{K+1}$, then the saddle point for $\bar{\Lambda}_K$ is not contained in $\bar{\Lambda}_{K+1}$. Since $\Lambda_K = \bar{\Lambda}_K - \bar{\Lambda}_{K+1}$, the saddle point for Λ is then contained in Λ_K. Since $\Lambda_K \cap \Lambda_J = \phi$ for $J \neq K$, there exists exactly one K such that (z_K, γ_K) belongs to Λ_K and is a saddle point for F over Λ. This index is uniquely specified, as shown, as the smallest integer K such that $C_K < C_{K+1}$, if such K exists. Otherwise, $C_1 = C_2 = \ldots = C_M$, and the saddle point belongs to Λ_M. □

3.2. Solutions to the Minimization Problem

In the following algorithm, we will derive a formal expression of the minimax solution for each Λ_K, $0 \leq K \leq M-1$, and give the necessary and sufficient conditions such that the solution exists. The procedure of searching for the saddle point solution is started from K = 0. If the solution in Λ_0 does not satisfy the necessary and sufficient conditions, the algorithm then searches Λ_1, and so on. We shall show that the solution reduces to finding the solution of a constrained minimization problem. By Lemma 4, a saddle point must exist.

Define

$$\Lambda_K = \{(z,\gamma): 0 = \gamma_1 = \gamma_2 = \ldots = \gamma_K < \gamma_{K+1} \leq \gamma_{K+2} \leq \ldots \leq \gamma_M$$

$$\sum_1^M \lambda_i \gamma_i \leq P_2;$$

$$z_1 \geq z_2 \geq \ldots \geq z_K \geq z_{K+1} \geq z_{K+2} \geq \ldots \geq z_M \geq 0.$$

$$\sum_1^M z_i \leq P_1\}$$

$$F(z,\gamma) = \frac{K}{2} \log (1+z_1) + \frac{1}{2} \sum_{K+1}^{M} \log \left(1+ \frac{z_i}{1+\gamma_i}\right)$$

$$= \frac{M}{2} \log (1+z_1) - \frac{1}{2} \sum_{K+1}^{M} \log (1+\gamma_i)$$

By Lemma 5 and Lemma 7, $z_i = z_1 - \gamma_i$, $i=K+1,\ldots,M$, so that

$$Kz_1 + \sum_{K+1}^{M} (z_1-\gamma_i) = Mz_1 - \sum_{K+1}^{M} \gamma_i = P_1.$$

Therefore, $$z_1 = \frac{P_1+\sum_{K+1}^{M}\gamma_i}{M}, \quad 1 + z_1 = \frac{M+P_1+\sum_{K+1}^{M}\gamma_i}{M} = \frac{K+P_1+\sum_{K+1}^{M}x_i}{M},$$

where we have defined $x_i \equiv 1+\gamma_i$, $i = K+1,\ldots,M$. This gives

$$\max_z F(z,\gamma) = F_1(x) = \frac{M}{2} \log \left(K+P+\sum_{K+1}^{M} x_i\right) - \tfrac{1}{2} \sum_{K+1}^{M} \log x_i - \frac{M}{2} \log M.$$

Our objective is to maximize $-F_1$ subject to

$$\sum_{K+1}^{M} \lambda_i x_i \leq P_2 + \sum_{K+1}^{M} \lambda_i, \tag{C_1}$$

$$1 < x_{K+1} \leq \cdots \leq x_M, \tag{C_2}$$

$$P_1 + \sum_{K+1}^{M} x_i \geq Mx_M - K. \tag{C_3}$$

Since F_1 is strictly concave and the constraints are convex, the minimization problem has a solution if and only if the Kuhn-Tucker conditions are satisfied; the solution, if it exists, is unique (see, e.g., Wismer and Chattergy (1978)).

Lemma 10: Λ_K will contain the saddle point for F if and only if K is the smallest integer $\leq M$ such that the above constrained minimization problem has a solution. When this occurs, and x^* is the solution, then (z^*,γ^*) is the saddle point, where

$$\gamma_i^* = x_i^* - 1, \qquad i = K+1,\ldots,M;$$

$$\gamma_i^* = 0 \qquad i \leq K \quad (\gamma_0^* \equiv 0);$$

$$z_i^* = (P_1 + \sum_{K+1}^{M} \gamma_i^*)/M - \gamma_i^* \qquad i = 1,2,\ldots,M.$$

Proof: If the minimization problem has a solution for some K, then the minimum equals $\underset{(z,\gamma)\in\Lambda_K}{\min_{\gamma} \max_{z}} F(z,\gamma)$. Since $\Lambda_K = \bar{\Lambda}_K - \bar{\Lambda}_{K+1}$, the minimizing point (z^*,γ^*) belongs to $\bar{\Lambda}_K$ but not to $\bar{\Lambda}_{K+1}$. Since $\bar{\Lambda}_K \supset \bar{\Lambda}_{K+1}$, this gives $C_K < C_{K+1}$, as defined in Lemma 9, and the result follows from Lemma 9. □

Using constrained optimization, define an objective functional as follows

$$\begin{aligned} L(\underline{x},\beta,\underline{\alpha}) = &- \frac{M}{2} \log (K + P_1 + \sum_{K+1}^{M} x_i) + \tfrac{1}{2} \sum_{K+1}^{M} \log x_i \\ &+ \frac{M}{2} \log M + \beta(P_2 + \sum_{K+1}^{M} \lambda_i - \sum_{K+1}^{M} \lambda_i x_i) \\ &+ \sum_{K+2}^{M} \alpha_i(x_i - x_{i-1}) + \alpha_{K+1}(x_{K+1} - 1) + \sigma(P_1 + \sum_{K+1}^{M} x_i - Mx_M + K). \end{aligned}$$

The Kuhn-Tucker conditions are as follows

$$- \frac{M}{2} \frac{1}{K+P_1+\sum_{K+1}^{M} x_i} + \frac{1}{2x_i} - \beta\lambda_i + \alpha_i - \alpha_{i+1} + \sigma = 0, \qquad (G_1)$$

$$i = K+1,\ldots,M-1$$

$$- \frac{M}{2} \frac{1}{K+P_1+\sum_{K+1}^{M} x_i} + \frac{1}{2x_M} - \beta\lambda_M + \alpha_M - \sigma(M-1) = 0 \qquad (G_2)$$

$$\beta(P_2 + \sum_{K+1}^{M} \lambda_i - \sum_{K+1}^{M} \lambda_i x_i) = 0; \quad P_2 + \sum_{K+1}^{M} \lambda_i - \sum_{K+1}^{M} \lambda_i x_i \geq 0$$

$$\alpha_i(x_i - x_{i-1}) = 0; \quad x_i - x_{i-1} \geq 0, \; K+2 \leq i \leq M,$$

$$\alpha_{K+1}(x_{K+1} - 1) = 0; \quad x_{K+1} - 1 > 0.$$

$$\sigma(P_1 + \sum_{K+1}^{M} x_i - Mx_M + K) = 0; \; P_1 + \sum_{K+1}^{M} x_i - Mx_M + K \geq 0.$$

All the parameters β, α_i and σ are non-negative. Note that α_{K+1} must be zero. We first show that $\sigma = \alpha_1 = \ldots = \alpha_M = 0$. Suppose $\sigma > 0$, so that $P_1 + \sum_{K+1}^{M} x_i + K = Mx_M$. (G_2) then reduces to

$$-\beta\lambda_M + \alpha_M - \sigma(M-1) = 0$$

$$\alpha_M = \beta\lambda_M + (M-1)\sigma > 0$$

This gives $x_M = X_{M-1}$, and by (G_1)

$$-\beta\lambda_{M-1} + \alpha_{M-1} - \alpha_M + \sigma = 0$$

$$\alpha_{M-1} = \beta(\lambda_M + \lambda_{M-1}) + (M-2)\sigma > 0.$$

Continuing in this way, one obtains

$$x_M = x_{M-1} = \ldots = x_{K+1}, \; \alpha_{K+1} = \beta(\lambda_M + \ldots + \lambda_{K+1}) + K\sigma.$$

$\alpha_{K+1} > 0$ contradicts $x_{K+1} > 1$. If $\alpha_{K+1} = 0$, then existence of a solution for $\sigma \neq 0$ requires that σ and β have opposite signs, a contradiction, provided that $K > 0$. If $K = 0$ and $\alpha_{K+1} = 0$, then existence of a solution requires $\beta = 0$. Thus, $\sigma = 0$ when $\beta > 0$.

Now suppose that $\beta > 0$ and $\alpha_M \neq 0$. Then $x_M = x_{M-1}$, and one obtains $-\beta(\lambda_{M-1} - \lambda_M) + \alpha_{M-1} - 2\alpha_M = 0$. β, $\alpha_{M=1}$ and α_M must each be strictly positive or zero, and $\lambda_{M-1} \geq \lambda_M$. If $\alpha_{M-1} = 0$, then $\alpha_M \neq 0$ implies α_M and β have opposite signs, a contradiction. Thus $\alpha_{M-1} \neq 0$ and $\alpha_{M-1} = 2\alpha_M + \beta(\lambda_{M-1} - \lambda_M)$.

Moreover, $x_{M-1} = x_{M-2} = x_M$. Thus

$$-\beta\lambda_{M-2} + \alpha_{M-2} - \alpha_{M-1} + \beta\lambda_M - \alpha_M = 0,$$

or $\quad -\beta(\lambda_{M-2}-\lambda_M) + \alpha_{M-2} - 3\alpha_M - \beta(\lambda_{M-1}-\lambda_M) = 0,$

giving $\quad -\beta(\lambda_{M-2}+\lambda_{M-1}-2\lambda_M) + \alpha_{M-2} - 3\alpha_M = 0.$

As above, this requires that $\alpha_{M-2} \neq 0$, so that $x_{M-2} = x_{M-3}$. Continuing in this way, one obtains $\alpha_i \neq 0$, for all $i \leq M$, contradicting $\alpha_{K+1} = 0$. Therefore, $\alpha_M \neq 0$. By similar arguments, $\alpha_{M-1}, \alpha_{M-2}, \ldots, \alpha_{K+1}$ must all equal to zero.

We now have $\sigma = \alpha_{K+1} = \ldots = \alpha_M = 0$ when $\beta > 0$. Inspecting the proof, one sees that this also holds when $\beta = 0$, provided that $K > 0$. If $K = 0$, then the proof shows (if $\beta = 0$) that $\sigma(i-1) = \alpha_i$, $i > 1$. Hence, the solution in this case is $x_1 = x_2 = \ldots = x_M$. However, we require that (since $\sigma \neq 0$) $P_1 + \Sigma_1^M x_i = Mx_M$, which cannot be satisfied by $x_1 = \ldots = x_M$ unless $P_1 = 0$. Thus, we see that $\sigma \neq 0$ is not possible unless $P_i = 0$. This completes the proof that (for $P_1 > 0$) $\sigma = \alpha_1 = \ldots = \alpha_M = 0$ is necessary in order that the minimization problem have a solution.

Assuming now that $\sigma = \alpha_1 = \ldots = \alpha_M = 0$, it is obvious that G_1 and G_2 have a solution for $\beta = 0$, provided that $K > 0$, given by $x_{K+1} = \ldots = x_M = (P_1+K)/K$. However, we also have the constraint $\Sigma_{K+1}^M \lambda_i x_i \leq P_2 + \Sigma_{i=K+1}^M \lambda_i$, which shows that for this constant solution to hold, it is necessary and sufficient that $P_1 \leq KP_2/\Sigma_{K+1}^M \lambda_i$.

Thus, Λ_K contains a solution to the minimization problem if $P_1 \leq KP_2/\Sigma_{K+1}^M \lambda_i$. If such K were the smallest integer i such that Λ_i yields a solution to the minimization problem, then this solution would give the saddle point (z^*, τ^*) for F on Λ, defined as follows:

$$\tau_i^* = 0 \qquad i \leq K$$

$$\tau_i^* = P_1/K \qquad i = K+1, \ldots, M$$

$$z_i^* = P_1/K \qquad i \leq K$$

$$= 0 \qquad i = K+1,\ldots,M.$$

We now assume that $P_1 > KP_2/\Sigma_{K+1}^{M}\lambda_i$, and that $\sigma = \alpha_{K+1} = \ldots = \alpha_M = 0$. Now ($G_1$) and ($G_2$) can be reduced to the following:

$$-\frac{M}{2}\frac{1}{K+P_1+\sum_{K+1}^{M} x_i} + \frac{1}{2x_i} - \beta\lambda_i = 0, \quad i=K+1,\ldots,M \tag{G_3}$$

Set $$\sum_{K+1}^{M} \lambda_i x_i = P_2 + \sum_{K+1}^{M} \lambda_i. \tag{G_4}$$

Multiplying through (G_3) by ($2x_i$), one has

$$\frac{-Mx_i}{K+P_1+\sum_{K+1}^{M} x_i} + 1 - 2\beta\lambda_i x_i = 0, \ i = K+1,\ldots,M. \tag{G_5}$$

Summing (G_5) over all i, we have

$$\frac{-M\sum_{K+1}^{M} x_i}{K+P_1+\sum_{K+1}^{M} x_i} + (M-K) - 2\beta(\sum_{K+1}^{M} \lambda_i x_i) = 0. \tag{G_6}$$

Put $y = \sum_{K+1}^{M} x_i$. Then

$$\beta = \frac{-My+(M-K)(K+P_1+y)}{2(P_2+\sum_{K+1}^{M} \lambda_i)(K+P_1+y)} \tag{G_7}$$

It can be seen that $\beta > 0$ is satisfied by G_7. To see this, one notes that the numerator of G_7 is always ≥ 0 since $P_1 + K + y \geq Mx_M$ is a constraint. Thus, $(M-K)(P_1+K) \geq (M-K)(Mx_M-y) \geq Ky$, since the last inequality is equivalent to

$M(\Sigma_{K+1}^{M}(x_M-x_i)) \geq 0$. This shows that the numerator is always non-negative, and that it is strictly positive unless $x_i = x_M$ for $i = K+1,\ldots,M$. However, this requires that $P_1 \leq KP_2/\Sigma_{K+1}^{M}\lambda_i$, and we are assuming that this inequality does not hold.

Returning to G_7,

$$2\beta(K+P_1+y) = \frac{(M-K)(K+P_1)-Ky}{P_2+\sum_{K+1}^{M}\lambda_j}. \qquad (G_8)$$

Substituting (G_8) in (G_5), one obtains

$$-Mx_i + (K+P_1+y) - \frac{[(M-K)(K+P_1)-Ky]\lambda_i x_i}{P_2+\sum_{K+1}^{M}\lambda_j} = 0 \qquad (G_9)$$

Thus

$$x_i = \frac{(P_2+\sum_{K+1}^{M}\lambda_j)(K+P_1+y)}{M(P_2+\sum_{K+1}^{M}\lambda_k) + [(M-K)(K+P_1)-Ky]\lambda_i}$$

$$= \frac{(P_2+\sum_{K+1}^{M}\lambda_j)(K+P_1+y)}{M[P_2+\sum_{K+1}^{M}\lambda_k+(P_1+K)\lambda_i] - K(K+P_1+y)\lambda_i} \qquad (G_{10})$$

where $y = \sum_{K+1}^{M} x_i$. Summing both sides of G_{10}, y is a solution of the equation

$$y = (P_2+\sum_{K+1}^{M}\lambda_j)\sum_{i=K+1}^{M}\frac{K+P_1+y}{M[P_2+\sum_{K+1}^{M}\lambda_k+(P_1+K)\lambda_i]-K(K+P_1+y)\lambda_i}. \qquad (G_{11})$$

Multiplying (G_{10}) by (λ_i) on both sides, and summing over all i, one obtains

$$K+P_1+y = \frac{1}{\displaystyle\sum_{K+1}^{M} \frac{\lambda_i}{M\left[P_2+\Sigma_{K+1}^{M}\lambda_i+(P_1+K)\lambda_i\right] - K(K+P_1+y)\lambda_i}}. \qquad (G_{12})$$

Substituting (G_{11}) in (G_{10})

$$x_i = \frac{P_2 + \displaystyle\sum_{K+1}^{M}\lambda_i}{M\left[P_2+\displaystyle\sum_{K+1}^{M}\lambda_i+(P_1+K)\lambda_i\right] - K(K+P_1+y)\lambda_i}$$

$$\times \frac{1}{\displaystyle\sum_{K+1}^{M} \frac{\lambda_i}{M\left[P_2+\Sigma_{K+1}^{M}\lambda_i+(P_1+K)\lambda_i\right] - K(K+P_1+y)\lambda_i}}. \qquad (G_{13})$$

Inspecting G_{10}, it can be seen that x_i is an increasing function of i, $K+1 \leq i \leq M$, since (λ_i) is a non-increasing sequence and $(P_1+K)(M-K) - Ky > 0$ when $P_1 > KP_2/\Sigma_{K+1}^{M}\lambda_i$.

Define the right side of G_{11} to be f(y); we now show that G_{11} yields a unique solution $y = f(y)$.

As previously shown, $(M-K)(K+P_1) - Ky \geq 0$, so $y \leq (M-K)(K+P_1)/K$. When equality holds in this relation, we have the solution $y_0 = (M-K)(K+P_1)/K$, which is the solution obtained when $P_1 \leq KP_2/\Sigma_{K+1}^{M}\lambda_i$. Hence, any solution y_1 of $y = f(y)$ must satisfy $y_1 \leq y_0$.

Differentiating f with respect to y, one obtains

$$f'(y) = \left[P_2+\sum_{K+1}^{M}\lambda_i\right]\sum_{i=K+1}^{M} \frac{M\left[P_2+\displaystyle\sum_{j=K+1}^{M}\lambda_j\right]+M(K+P_1)\lambda_i}{\left[M\left[P_2+\displaystyle\sum_{k=K+1}^{M}\lambda_k\right]+\lambda_i\left[[M-K](K+P_1)-Ky\right]\right]^2}.$$

f' is clearly strictly positive, since $(M-K)(K+P_1) \geq Ky$.

Thus $f'(y) > 0$ for $y \leq y_0$. Also, setting $y = y_0 = (M-K)(K+P_1)/K$, one sees that $f(y_0) = (M-K)(K+P_1+y_0)/M = y_0$.

Now $f(0) > 0$ and $f(y_0) = y_0$. Thus, there will be a solution of $y = f(y)$ for $y < y_0$ if $f'(y) > 1$ in a neighbor-hood of y_0. Evaluating $f'(y)$ at $y = y_0$, we obtain

$$f'(y_0) = \left[P_2 + \sum_{K+1}^{M} \lambda_i\right] \sum_{i=K+1}^{M} \frac{M\left[P_2 + \sum_{k=K+1}^{M} \lambda_k\right] + M(K+P_1)\lambda_i}{M^2\left[P_2 + \sum_{s=K+1}^{M} \lambda_s\right]^2}$$

$$= \frac{M-K}{M} + \frac{(K+P_1) \sum_{j=K+1}^{M} \lambda_j}{M\left[P_2 + \sum_{s=K+1}^{M} \lambda_s\right]} .$$

This shows that $f'(y_0) > 1$ if and only if

$$(K+P_1) \sum_{j=K+1}^{M} \lambda_j \geq K\left[P_2 + \sum_{i=K+1}^{M} \lambda_i\right]$$

which holds if and only if

$$P_1 > KP_2 / \sum_{i=K+1}^{M} \lambda_i .$$

We have now shown that a solution $y = f(y)$ must exist for $y < y_0$, when $P_1 > KP_1/\Sigma_{i=K+1}^{M}\lambda_i$. We claim that there exists exactly one such solution. For this, it is sufficient to show that $f''(y) > 0$ for $0 < y < y_0$. This is clear by inspection of the above expression for $f'(y)$.

Thus, we have that a unique solution of $y = f(y)$ exists for $y < y_0$, when $P_1 > KP_2/\Sigma_{i=K+1}^{M}\lambda_i$.

We now have $\{x_i, i \leq M\}$ defined in terms of $P_1, P_2, K, M, \{\lambda_i, K+1 \leq i \leq M\}$, and y, where $y = \Sigma_{i=K+1}^{M} x_i$ and y must be a solution of G_{11}. Any solution (x_n)

to the minimization problem must satisfy the constraints: $x_{K+1} > 1$; $x_{i+1} \geq x_i$; $i \leq M-1$; $P_1 + K + \Sigma^M_{i=K+1} x_i \geq Mx_M$; and $P_2 + \Sigma^M_{i=K+1}\lambda_i \geq \Sigma^M_{j=K+1}\lambda_j x_j$. When $P_1 > KP_2/\Sigma^M_{i=K+1}\lambda_i$, a solution requires the parameter β in G_3 to be non-zero, and this requires that $P_2 + \Sigma^M_{i=K+1}\lambda_i = \Sigma^M_{j=K+1}\lambda_j x_j$. Inspection of G_{13} shows that this equality is satisfied by (x_i) as defined in G_{10} (and G_{13}). Also, G_{10} shows that (x_i) is non-decreasing. The constraint $P_1 + K + \Sigma^M_{i=K+1}x_i \geq Mx_M$ is satisfied when $(x_{K+1}, \ldots, x_M)$ is defined by G_{10} (or G_{13}); to verify this, one can inspect G_9. If $P_1 > KP_2/\Sigma^M_{i=K+1}\lambda_i$, then, as previously shown, $(M-K)(K+P_1)-Ky > 0$. G_9 then shows that $K+P_1+y > Mx_M$. Thus, when $P_1 > KP_2/\Sigma^M_{i=K+1}\lambda_i$, then Λ_K contains a solution to the minimization problem, given by G_{10} (and G_{13}), provided only that $X_{K+1} > 1$.

To obtain a solution, one begins with Λ_0. If the condition $x_1 > 1$ is not satisfied by Λ_0, then Λ_0 is not admissible, and one proceeds to Λ_1. If $P_1 > P_2/\Sigma^M_{i=2}\lambda_i$ and $x_2 \leq 1$, then Λ_1 is not admissible. One then proceeds to Λ_2, and continues in this way up to the first K such that either $P_1 \leq KP_2/\Sigma^M_{i=K+1}\lambda_i$ or else $P_1 > KP_2/\Sigma^M_{i=K+1}\lambda_i$ and $x_{K+1} > 1$.

We summarize this development, and the major results, in the following theorem.

Theorem 1:

(1) The minimization problem will have a solution in Λ_K if and only if one of the following conditions is satisfied:

a) $$P_1 \leq KP_2/\sum_{i=K+1}^{M}\lambda_i$$

b) $$P_1 > KP_2/\sum_{i=K+1}^{M}\lambda_i, \quad \text{and} \quad x_{K+1} > 1,$$

where x_{K+1} is defined by G_{10} (and G_{13}).

(2) When the minimization problem has a solution γ^* in Λ_K, then $F_0(\gamma^*)$ has the following values:

a) If $P_1 \leq KP_2/\sum_{i=K+1}^{M} \lambda_i$, then $F_0(\gamma) = \frac{K}{2}\log[1 + P_1/K]$.

b) If $P_1 > KP_2/\sum_{i=K+1}^{M} \lambda_i$, then

$$F_0(\gamma) = \frac{M}{2}\log\left[\frac{P_1 + M + \sum_{i=K+1}^{M} x_i}{M}\right] + \frac{1}{2}\sum_{i=K+1}^{M}\log\left[\frac{P_1 + M + \sum_{j=K+1}^{M} x_i}{Mx_i}\right]$$

where $\{x_i,\ i=K+1,\ldots,M\}$ is defined by G_{10} (or G_{13}).

3.3. Information Capacity

Essentially, the minimization problem in Λ_K has two classes of solutions: one is when $P_1 + \Sigma_{i=K+1}^{M} x_i + K = Mx_M$ (in this case, $P_2 + \Sigma_{i=K+1}^{M}\lambda_i \geq \Sigma_{i=K+1}^{M}\lambda_i\gamma_i$); the second is when $P_2 + \Sigma_{i=K+1}^{M}\lambda_i = \Sigma_{i=K+1}^{M}\lambda_i\gamma_i$ (in this case $P_1 + \Sigma_{i=K+1}^{M} x_i + K \geq Mx_M$). However, we shall now show that only one solution can define a saddle point for F over Λ.

Lemma 11:

(1) If the minimization problem in Λ_K has a solution x^* such that $F_0(x^*)$ is the saddle value for F on Λ, then $P_1 > KP_2/\Sigma_{i=K+1}^{M}\lambda_i$.

(2) The saddle value of $F(z^*,\gamma^*)$ of F on Λ satisfies

$$F(z^*,\gamma^*) < \frac{K}{2}\log[1 + P_1/K]$$

where $K \leq M$ is the smallest integer satisfying $P_1 \leq KP_2/\Sigma_{i=K+1}^{M}\lambda_i$. If no such K exists, then

$$F(z^*,\gamma^*) < \frac{M}{2}\log\left[\frac{P_2 + \lambda_M(M+P_1)}{M\lambda_M}\right] - \frac{1}{2}\log\,[P_2/\lambda_M].$$

Proof: (1) If the minimization problem has a solution x^* in Λ_K which defines the saddle point (z^*,γ^*) for F on Λ, then (z^*,γ^*) has the form:

$$\begin{aligned}\gamma_i^* &= 0 && i \le K\\ &= x_i^* - 1 && i \ge K+1\\ z_i &= \frac{P_1 + \Sigma_{j=1}^{M}\gamma_j^*}{M} - \gamma_i^* && i \ge 1.\end{aligned}$$

When $P_1 \le KP_2/\Sigma_{i=K+1}^{M}\lambda_i$, then a solution exists for the minimization problem, defined by

$$\begin{aligned}x_i^* &= 1, && i \le K\\ x_i^* &= (P_1+K)/K && i \ge K+1,\end{aligned}$$

giving

$$\begin{aligned}z_i^* &= \frac{P_1 + (M-K)P_1/K}{M} && i \le K\\ &= \frac{P_1 + (M-K)P_1/K}{M} - P_1/K && i \ge K+1.\end{aligned}$$

Thus

$$\begin{aligned}z_i^* &= P_1/K && i \le K\\ &= 0 && i \ge K+1.\end{aligned}$$

Inserting these values into the definition of F (or using $F_0(x^*)$, one obtains

$$F(z^*,\gamma^*) = \frac{K}{2}\log[1 + P_1/K].$$

Now, in order for this to be a saddle value for F, it is necessary that it satisfy $F(z^*,\gamma^*) \le F(z^*,\gamma)$ for all admissible γ. Thus we obtain the requirement that

$$\frac{K}{2}\log[1 + P_1/K] \le \frac{1}{2}\sum_{i=1}^{K}\log\left[1 + \frac{P_1}{K(1+\gamma_i)}\right]$$

for all sequences (γ_i) such that $0 \le \gamma_i$, $1 \le i \le M$, $\Sigma_{i=1}^{M}\lambda_i\gamma_i \le P_2$. It is obvious that this cannot hold. Thus, the saddle value cannot be obtained from a solution of the minimization problem in Λ_K when $P_1 \le KP_2/\Sigma_{i=K+1}^{M}\lambda_i$.

The saddle value $F(z^*,\gamma^*)$ is the minimax value for the jammer. Thus, if K is the smallest integer such that the minimization problem has a solution in Λ_K, then by part (1), $P_1 > KP_2/\Sigma_{i=K+1}^{M}\lambda_i$. Now, $\Lambda_K = \bar{\Lambda}_K - \bar{\Lambda}_{K+1}$, as defined in Lemma 8. Thus, $\Lambda_{K+1} \subset \bar{\Lambda}_{K+1} \subset \bar{\Lambda}_K$. The solution to the minimization problem in Λ_K gives a minimax solution for the jammer in $\bar{\Lambda}_K$, whose value is C_K. We have, by Lemma 8, $C_K \le C_{K+1}$. Hence, if $P_1 \le KP_2/\Sigma_{i=K+1}^{M}\lambda_i$, then $C_K = \frac{K}{2}\log[1 + P_1/K]$, as shown in the proof of part (1), and so the saddle value is strictly less than $K/2 \log[1 + P_1/K]$.

If Λ_M contains the saddle point, then $\gamma_1 = \ldots\gamma_{M-1} = 0$, and γ_M must satisfy $\gamma_M\lambda_M \le P_2$. Since Λ_M always contains the solution $\gamma_m = P_2/\lambda_M$ to the minimization problem, the resulting value of $F_0(\gamma)$ is always an upper bound on the saddle value of F on Λ. □

<u>Lemma 12</u>: Λ_K contains a solution to the minimization problem if

$$P_2 > \sum_{i=K+1}^{M}(\lambda_{K+1} - \lambda_i)\,\frac{[(M-K)(P_1+K) - Ky]\lambda_i/M}{P_2 + \Sigma_{K+1}^{M}\lambda_i + [(M-K)(P_1+K) - Ky]\lambda_i/M} \qquad (*)$$

This always holds when $P_2 \ge \Sigma_{i=K+1}^{M}(\lambda_{K+1} - \lambda_i)$.

<u>Proof</u>: We can assume that $P_1 > KP_2/(\Sigma_{j=K+1}^{M}\lambda_j)$. We then must only show that $x_{K+1} > 1$ holds if

$P_2 \geq \Sigma^M_{i=K+1}(\lambda_{K+1} - \lambda_i)[D_i - M(P_2 + \Sigma^M_{K+1}\lambda_j)]/D_i$, where

$$D_i = M\left[P_2 + \sum_{j=K+1}^{M} \lambda_j\right] + [(M-K)[P_1+K] - Ky]\lambda_i .$$

Applying G_{13}, $x_{K+1} > 1$ if and only if $P_2 + \Sigma^M_{i=K+1}\lambda_i > D_{K+1}\Sigma^M_{i=K+1}(\lambda_i/D_i)$. The right side can be written as $\Sigma^M_{i=K+1}(Q_i/D_i)$, where

$$Q_i = \lambda_{K+1}\left[M\left[P_2 + \sum_{j=K+1}^{M} \lambda_j\right] + [(M-K)(P_1+K) - Ky]\lambda_j\right]$$

$$+ \lambda_i M\left[P_2 + \sum_{k=K+1}^{M} \lambda_k\right] - \lambda_{K+1}\left[P_2 + \sum_{k=K+1}^{M} \lambda_k\right]$$

$$= \lambda_{K+1}D_i + (\lambda_i - \lambda_{K+1})\left[P_2 + \sum_{k=K+1}^{M} \lambda_k\right].$$

Hence, $x_{K+1} > 1$ if and only if

$$P_2 + \sum_{j=K+1}^{M} \lambda_j > (M-K)\lambda_{K+1} + \sum_{i=K+1}^{M} \frac{M(\lambda_i - \lambda_{K+1})\left[P_2 + \sum_{k=K+1}^{M} \lambda_K\right]}{D_i}.$$

That is, if and only if (*) holds. Since $\lambda_i \leq \lambda_{K+1}$ for $i \geq K+1$, and $D_i > 0$ for $i \leq M$, this yields the desired result:

$$P_2 + \sum_{j=K+1}^{M} \lambda_j \geq (M-K)\lambda_{K+1} \quad \text{implies } x_{K+1} > 1.$$

Note that if $\lambda_i = \lambda_{K+1}$ for $i \geq K+1$, then (*) is obviously satisfied and of course in this case $(P_2 > 0)$ $P_2 > \Sigma^M_{j=K+1}(\lambda_{K+1} - \lambda_j) = 0$. □

Lemma 12 gives the necessary and sufficient conditions for Λ_K to contain the saddle point of F on Λ. That is , K is the smallest integer such that the inequality (*) of Lemma 12 is satisfied. Lemmas 11 and 12 also give easily-verified bounds on the value of such K. That is, by Lemma 11, K must be less than the smallest integer k (if such k exists) satisfying $P_1 \leq kP_2/\Sigma_{i=k+1}^{M}\lambda_i$. For example, if $P_1 \leq P_2/\Sigma_{i=2}^{M}\lambda_i$, then Λ_0 must contain the saddle point.

Moreover, $K \leq k$, where k is the smallest integer such that $P_2 > \Sigma_{i=k+1}^{M}(\lambda_{k+1}-\lambda_i)$. Of course, this inequality is always satisfied for $k = M$.

We summarize the foregoing in the following main theorem.

Theorem 2: The saddle point of F on Λ is defined by the solution of the minimization problem in Λ_K, where K is the smallest integer such that a solution exists. If $\Lambda_0, \ldots, \Lambda_{K-1}$ does not contain a solution to the minimization problem, then Λ_K will contain a solution if and only if $\{x_i, i \geq K+1\}$, as defined in G_{10} (or G_{13}), satisfies $x_{K+1} > 1$. This is determined by the smallest value of K such that the inequality (*) of Lemma 12 is satisfied. A sufficient condition for this inequality to hold is that $P_2 \geq \Sigma_{i=K+1}^{M}(\lambda_{K+1}-\lambda_i)$. K must be smaller than the smallest integer k satisfying $P_1 \leq kP_2/\Sigma_{i=K+1}^{M}(\lambda_{K+1}-\lambda_i)$, if such an integer exists; in this case, the saddle value satisfies

$$F(z^*,\gamma^*) < \frac{k}{2}\log(1 + P_1/k).$$

If no such integer k exists, then

$$F(z^*,\gamma^*) < \frac{M}{2}\log\left[\frac{P_2 + \lambda_M(M+P_1)}{M\lambda_M}\right] - \tfrac{1}{2}\log\left[P_2/\lambda_M\right].$$

When Λ_K contains the saddle point, then it is given by

$$\gamma_i = 0, \quad i \leq K.$$

$$\gamma_i = \frac{\left[P_2 + \sum_{j=K+1}^{M}\lambda_j\right](K+P_1+y)}{M\left[P_2 + \sum_{k=K+1}^{M}\lambda_k + (P_1+K)\lambda_i\right] - K(K+P_1+y)} - 1, \qquad i \geq K+1.$$

where $$y = [P_2 + \sum_{K+1}^{M} \lambda_i] \sum_{K+1}^{M} \frac{K + P_1 + y}{M[P_2 + \sum_{K+1}^{M} \lambda_i + (P_1+K)\lambda_i] - K(K+P_1+y)\lambda_i}.$$

$$z_1 = \frac{P_1 + \sum_{K+1}^{M} \gamma_i}{M} = z_2 = \dots = z_K.$$

$$z_i = z_1 - (1+\gamma_i), \quad i = K+1, \dots, M.$$

$$F(z,\gamma) = \frac{M}{2} \log(1+z_1) - \frac{1}{2} \sum_{K+1}^{M} \log(1+\gamma_i).$$

When Λ_0 is admissible,

$$\gamma_i = \frac{P_2 + TrR_W}{P_2 + TrR_W + P_1\lambda_i} \frac{1}{\sum_{i=1}^{M} \frac{\lambda_i}{P_2 + TrR_W + P_1\lambda_i}} - 1,$$

$$z_i = \frac{P_1 + \sum_{j=1}^{M} \gamma_j}{M} - \gamma_i, \quad i=1,2,\dots;M$$

$$F(z,\gamma) = \frac{1}{2} \Sigma_1^M \log\left(1 + \frac{P_1\lambda_i}{P_2 + TrR_W}\right).$$

<u>Remark</u>: As seen from Theorem 1, the capacity of this channel without jamming is $\frac{M}{2} \log(1 + P_1/M)$. For a sense of the degradation that can be caused by an intelligent jammer, suppose that the saddle point lies in Λ_0. Then the saddle value, or the capacity when the jammer chooses his minimax strategy, is

$$F(z,\gamma) = \frac{M}{2} \log\left(1 + \frac{P_1}{M}\right) - \frac{1}{2} \sum_{i=1}^{M} \log\left[\frac{(P_2+TrR_W)(M+P_1)}{(P_2+TrR_W+P_1\lambda_i)M}\right]$$

$$= \frac{M}{2} \log\left(1 + \frac{P_1}{M}\right) - \frac{1}{2} \sum_{i=1}^{M} \log\left[\frac{M + P_1}{\left[1 + \frac{P_1\ \lambda_i}{P_2+TrR_W}\right]M}\right].$$

We now list some immediate consequences of Theorem 2, which are of interest in classical engineering applications.

Corollary 1: Suppose that one uses the constraint $E_{\mu_J} \|x\|_W^2 \leq P_2$ for the jammer. The saddle point solution is then given by Theorem 2, setting $\lambda_1 = \lambda_2 = \ldots = \lambda_M = 1$. The saddle point solution (z,γ) is contained in Λ_0, and has the form:

$$\gamma_i = \frac{P_1}{M} \qquad i = 1,2,\ldots,M$$

$$z_i = \frac{P_1 + P_2}{M} - \frac{P_2}{M} = \frac{P_1}{M} \qquad i = 1,2,\ldots,M.$$

Thus, the saddle value of F is

$$F(z,\gamma) = \frac{M}{2} \log\left[\frac{P_2 + P_1 + M}{P_2 + M}\right] = \frac{M}{2} \log\left[1 + \frac{P_1}{P_2 + M}\right].$$

Proof: The constraint on S is Trace $S = \Sigma_1^M \gamma_i \leq P_2$. Since (λ_i) affects the solution only through this constraint, the result follows.

Corollary 2: Consider the discrete-time memoryless Gaussian channel: $W = \mathrm{diag}[\lambda_1,\ldots,\lambda_M]$. With the constraints $\Sigma_{i=1}^M \lambda_i^{-1} z_i \leq MP_1$, $\Sigma_{j=1}^M \gamma_j \leq MP_2$, the optimum jamming signal has covariance matrix $\mathrm{diag}[\gamma_1,\ldots,\gamma_M]$, with (γ_i), (z_i), and the saddle value defined as in Theorem 2. If $\lambda_i = \lambda$, $i = 1,\ldots,M$, then these quantities are defined as in Corollary 1, substituting $M\lambda P_1$ and MP_2 for P_1 and P_2, respectively.

Proof: The first part is obvious, since R_W has the natural basis vectors (e_n) as eigenvectors, i.e., $e_n(j) = \delta_{nj}$. The second part results from the constraint $\Sigma_{i=1}^n z_i \leq n\lambda P_1$.

4. COMMENTS ON PRIOR RELATED WORK

We give a brief summary of Borden, Mason, and McEliece (1985). In that paper, the jamming channel is formulated as a two person game with mutual information as the payoff function. Their model is the one-dimensional additive channel, $Y = X + Z$; Y is the output; X the input, Z the noise. X and Z are independent random variables. $I(X;Y)$ is the mutual information between X and Y. $I(X;Y)$ is determined by X (coder) and Z (jammer), so they use $\phi(X,Z) \equiv I(X;Y)$ to express the payoff function. Under the assumption that the "signal to noise" ratio $EX^2/EZ^2 = A$ is fixed, they considered four cases which are distinguished by whether the input and/or output are subject to some quantization (binary quantization). They derived some results in each case.

When the channel is additive Gaussian, McEliece and Stark (1981) get the result, if there is no quantization on input and output, that the saddle point is obtained when both X and Z are Gaussian. Using the above notation, they obtain $\phi(X_0;Z_0) = \frac{1}{2}\log(1+A)$, $X_0 \sim N(0,EX_0^2)$, $Z_0 \sim N(0,EZ_0^2)$, $EX_0^2/EZ_0^2 = A$. One can obtain this from Theorem 2.13, using $M = 1$, $EZ^2 = 2A$, $EJ^2 = 1$.

5. GENERAL DISCUSSION

Either in mismatched or in jamming matched models, it is assumed that the coder recognized the eigenvectors of R_N, the covariance matrix for the additive noise. This is needed so that he can choose $R_{AX} = \Sigma_i \tau_n [R_N^{\frac{1}{2}} v_i] \otimes [R_N^{\frac{1}{2}} v_i]$, and the average mutual information can be expressed as $\frac{1}{2}\Sigma_i \log(1 + x_i^2(1+\gamma_i)^{-1})$. The jammer knows this solution; he will use the energy saving principle so that the coder can not attain any capacity above the minimax quantity. Actually, the jamming matched Gaussian channel is considered in two steps, that is.

$$\min_{\substack{(\alpha_i)\\ \alpha_i=\Sigma\lambda_i a_{ij}^2}} \;\min_{\substack{(\tau_i)\\ \Sigma\alpha_i\tau_i=P_2}} \;\max_{\substack{(z_i)\\ \Sigma z_i=P_1}} R(z,\tau)$$

$$= \min_{\substack{(\tau_i)\\ \Sigma\lambda_i\tau_i=P_2}} \;\max_{\substack{(z_i)\\ \Sigma z_i=P_1}} R(z,\tau) \qquad \text{(energy saving principle)}$$

$$= \max_{\substack{(z_i)\\ \Sigma z_i=P_1}} \;\min_{\substack{(\tau_i)\\ \Sigma\lambda_i\tau_i=P_2}} R(z,\tau) \qquad \text{(minimax theorem).}$$

The necessary and sufficient conditions for both the coder and the jammer to determine their saddle point strategies are that they both have full knowledge of the ambient Gaussian noise added in the channel, and that they know the opponent's energy constraint. That is, the jammer knows the value of P_1; the coder knows the value of P_2.

If the opponent's energy constraint is unknown, and is subject to a random distribution over an interval in $\mathbb{R}^+$, several variations can be considered. If the interval is bounded, then a minimax strategy for the player is to assume that his opponent will take the largest energy with probability one. The minimax information capacity is then simply obtained by using that largest right-hand boundary value as the energy constraint. If the interval is unbounded, a Bayesian approach seems reasonable to consider. Our result can then be used as a conditional objective function when P_1 and P_2 are given. The information capacity will be equal to the expectation with respect to the random variables P_1 and/or P_2.

REFERENCES

Baker, C.R. (1978). Capacity of the Gaussian channel without feedback. *Inform. and Control*, 37, 70-79.

__________ (1987a). Capacity of the mismatched Gaussian channel, *IEEE Trans. Information Theory*, IT-33, 802-812.

__________ and I.F. Chao (1989). Information capacity of the matched Gaussian channel with jamming, II. Infinite-dimensional channels (to appear).

Barbu and Precupanu (1986). (The list you gave me is Chao's thesis reference list and Barbu/Pre. isn't on it.

Borden, J.M., Mason, D.M. and McEliece, R.J. (1985). Some information theoretic saddle points. SIAM *J. of Control & Optim.*, vol. 23, No. 1, 129-143.

Danskin, J.M. (1967). *The Theory of Max-Min*. Springer-Verlag, New York.

Fan, K. (1951). Maximum properties and inequalities for the eigenvalues of completely continuous operators. *Proc. Nat. Acad. Sci.*, vol. 37, 760-766.

Ihara, S. (1978). On the capacity of channels with additive non-Gaussian noise, *Inform. and Control*, 37, 34-39.

McEliece, R.J. and Stark, W.E. (1981). An information theoretic study of communication in the presence of jamming. *Proc. 1981 IEEE Halt. Conf. on Comm.* Denver, Colorado, June 15-18.

McEliece, R.J. (1983). Communications in the presence of jamming - An introductory theoretic approach, in *Secure Digital Communications*. Spring-Verlag, 127-166.

McKeague, I.W. and Baker, C.R. (1986). The coding capacity of mismatched Gaussian channels. *IEEE Trans. Information Theory*, IT-32, 431-436.

Roberts, A.W., and Varberg, D.E. (1973). *Convex Functions*. Academic Press, New York.

Wismer, D.A. and Chattergy, R. (1978). *Introduction to Nonlinear Optimization: A Problem Solving Approach*. North-Holland, New York.